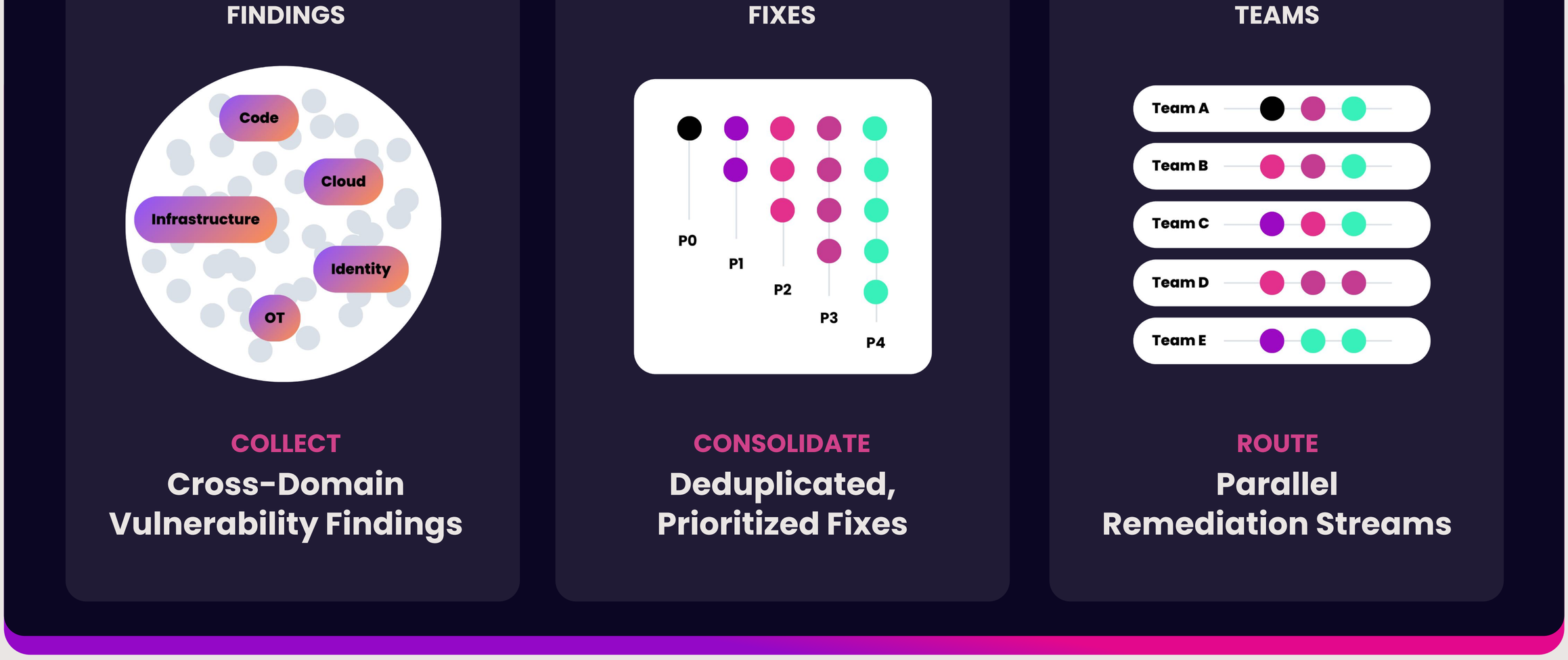
Prioritize Vulnerability Remediation Efforts with Seemplicity

SOLUTION BRIEF

Prioritizing vulnerability and exposure findings is essential to maximizing remediation impact, especially when balancing limited security team resources and busy development and operations team schedules. Seemplicity improves this process by prioritizing fixes rather than findings, giving you the ability to remediate your findings backlog more efficiently. Our platform incorporates business and technical context to identify what should take priority in your environment, ensuring that the most critical issues are addressed first.



The Problem with Traditional Findings-Based Scoring

Traditional vulnerability prioritization and management tools focus on findings, leaving security teams to struggle with:

AMBIGUOUS PRIORITIZATION

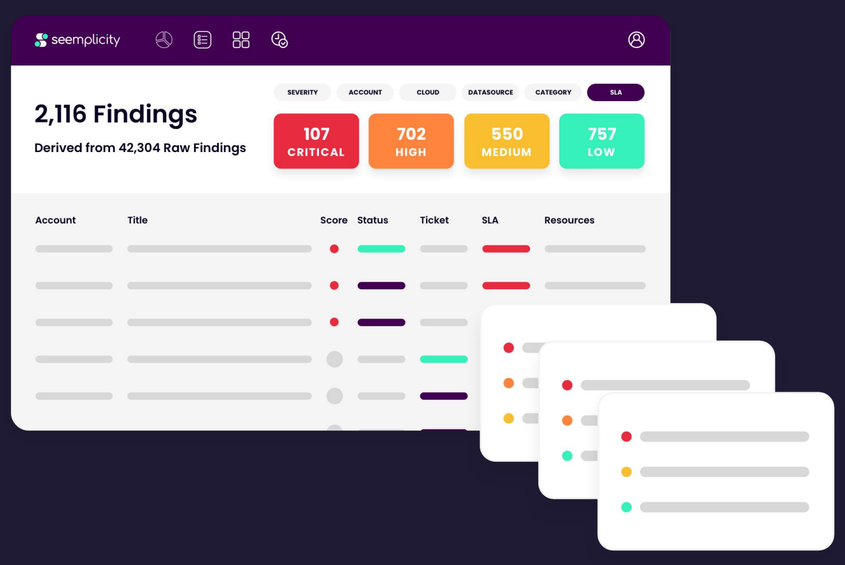
Most scanning and prioritization tools assign scores without clear rationale, making it difficult to explain to remediation teams why one vulnerability deserves priority over another.

EXTERNAL DEPENDENCY

Scanning and prioritization tools often rely on generalized external information such as threat intelligence and industry-standard scores, ignoring internal context and the specific needs of your organization.

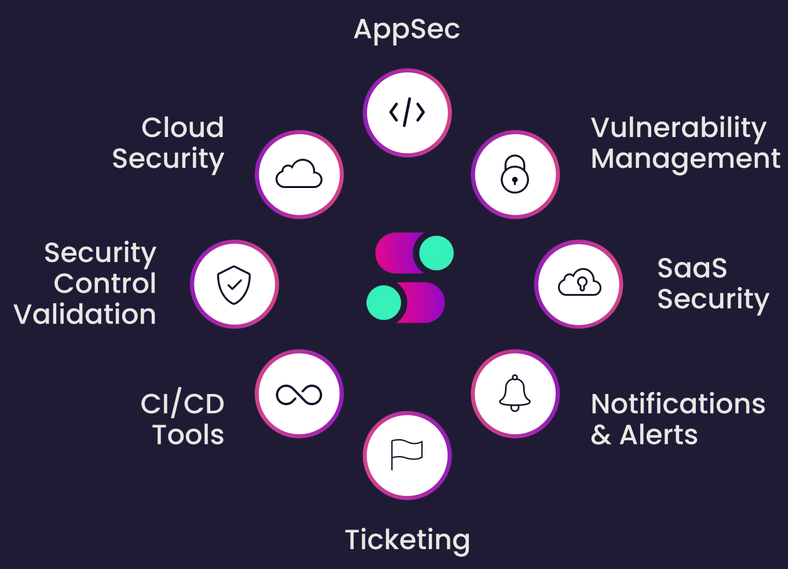
Choice Engine: Tailored Remediation Plans

The Seemplicity Choice Engine shifts the focus from individual findings to comprehensive remediation plans:



ACTION-ORIENTED PRIORITIZATION

Seemplicity prioritizes what needs to be fixed based on the impact of the remediation action; each fix typically addresses multiple findings.



INTEGRATED DATA

Seemplicity combines data from vulnerability tools, including internal business and technical context, along with external vulnerability intelligence associated with findings.

Comprehensive Context Integration

Seemplicity's prioritization process is enhanced with both internal and external context. Incorporating internal context, such as mission-critical business units, geographic regions, or regulated systems, allows for customized treatment of the organization's assets. This enables the Seemplicity platform to deliver tailored remediation plans that align with the priorities and risk profiles of each organization, ensuring that the most valuable and vulnerable assets receive prioritized attention.

For external context, Seemplicity leverages a wealth of intelligence to inform prioritization plans. This includes sources such as CISA's Known Exploited Vulnerabilities (KEV), VulnCheck KEV, threat intelligence feeds, and Exploit Prediction Scoring System (EPSS) percentages. By incorporating external insights, Seemplicity ensures that remediation plans are informed by the latest threat landscape to help organizations stay ahead of emerging risks that could impact their security posture.

EXTERNAL INTELLIGENCE SOURCES:

- CISA KEV
- VulnCheck KEV
- Threat Intelligence Feeds
- EPSS percentages
- Specific vulnerability types (Remote Code Execution (RCE), Privilege Escalation, etc.)

Scoring Rules and Customization

Every organization is unique, and so are its security needs. Seemplicity's tailored remediation plans incorporate:

TEAM-SPECIFIC PRIORITIZATION

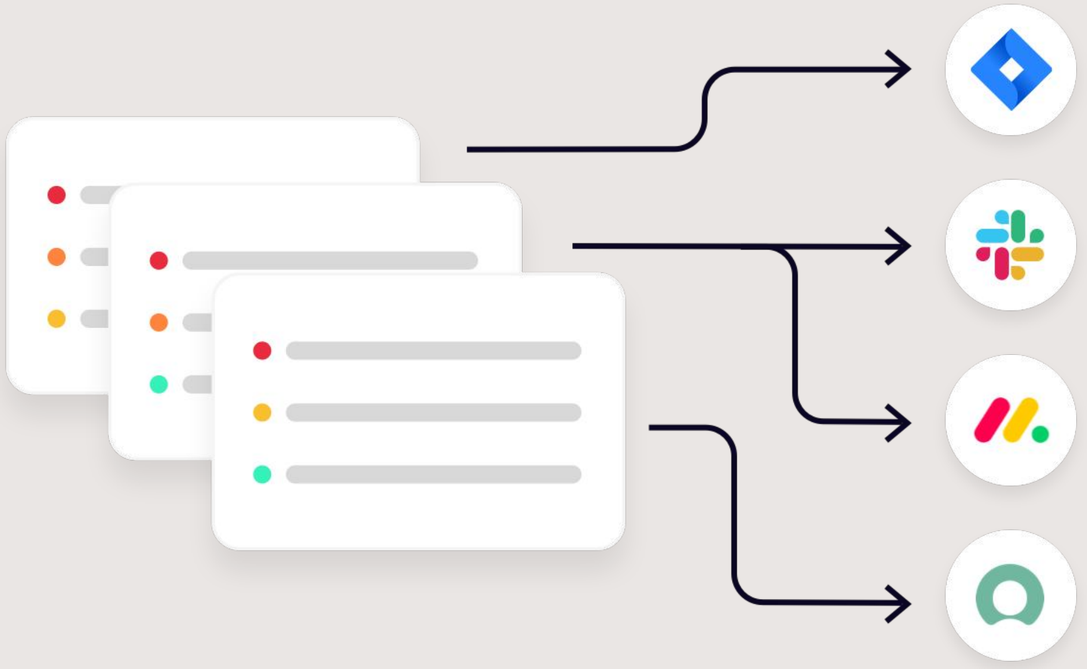
The Seemplicity Platform allows for customized prioritization of each remediation team's queue, incorporating scanner data from cloud misconfigurations, AppSec findings, and more.

CUSTOM SCORING RULES

Users can adjust scoring rules or assign fixed values tailored to their organization's priorities.

MANUAL ADJUSTMENTS

If desired, users can manually tweak priority across the platform to reflect real-time insights and urgent needs.



Beyond Prioritization

Prioritization is just the beginning. Seemplicity remediation plans also:

AUTOMATE WORKFLOWS

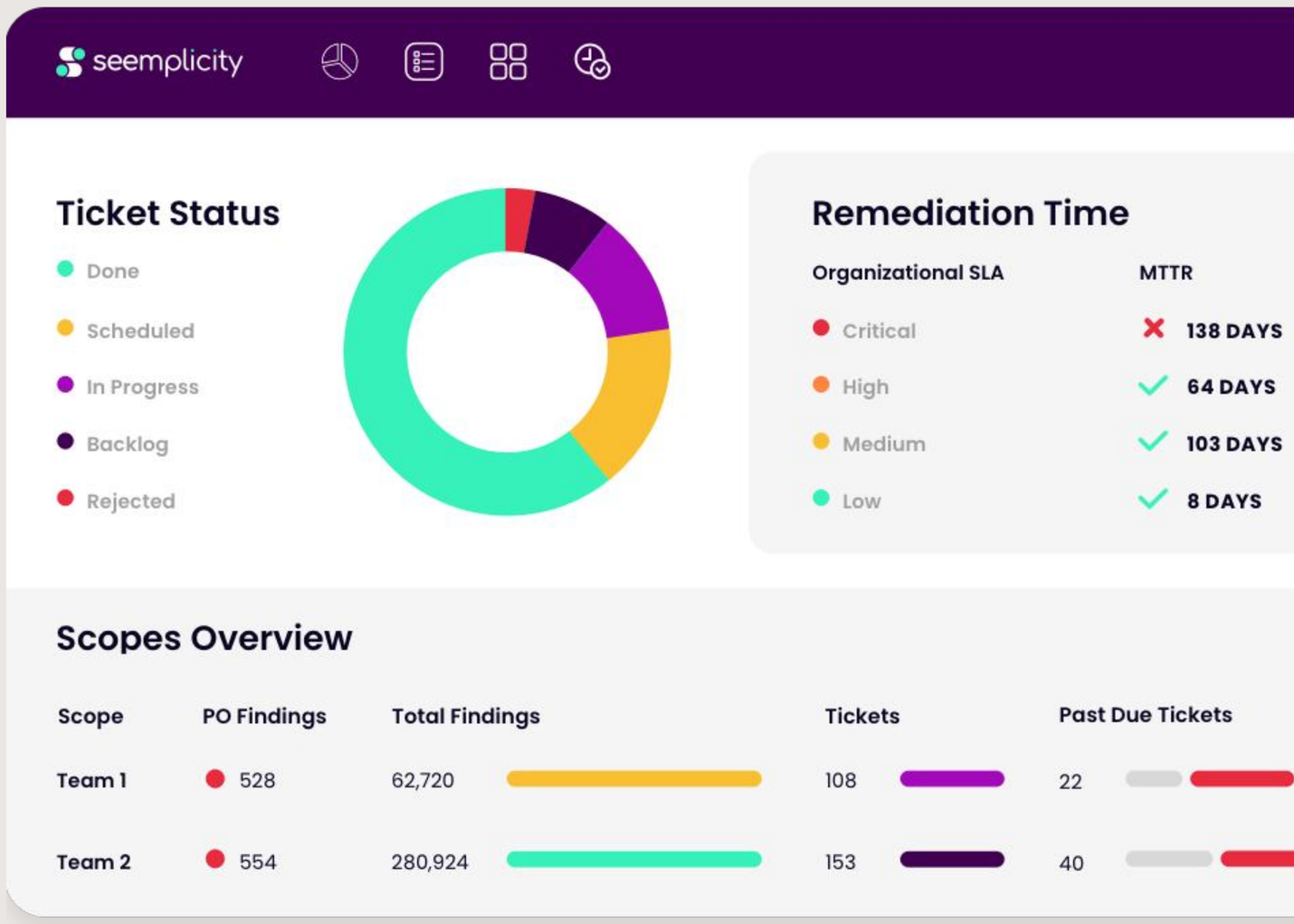
Seemplicity allows users to build out and set conditions for automated workflows, resulting in faster Mean Time to Remediation (MTTR).

ENHANCE PRODUCTIVITY

Fixing teams are assisted by Seemplicity's automated processes, receiving applicable vulnerability context and remediation instruction, all within their desired ticketing and work management platforms.

TRACK PROGRESS

Remediation progress is monitored to ensure timely resolution of vulnerabilities, accurate reporting and stakeholder visibility.



Don't Stop at Prioritization

The Seemplicity Choice Engine redefines vulnerability management prioritization by focusing on remediation actions. Don't just prioritize findings—transform your approach to security management with Seemplicity remediation plans.

For more information about Seemplicity's Platform for Remediation Operations, watch our on-demand demo video to see how it can revolutionize your vulnerability and exposure management strategy.

WATCH ON-DEMAND DEMO